Gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la CLI

ONTAP 9

NetApp
April 24, 2024

Sommario

Gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la CLI

Gestisci la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la panoramica CLI

È possibile gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su macchine virtuali storage (SVM) utilizzando la CLI.

È possibile gestire la sicurezza dei file NTFS e le policy di controllo dai client SMB o utilizzando la CLI. Tuttavia, l'utilizzo della CLI per configurare le policy di controllo e sicurezza dei file elimina la necessità di utilizzare un client remoto per gestire la sicurezza dei file. L'utilizzo della CLI può ridurre significativamente il tempo necessario per applicare la protezione a molti file e cartelle utilizzando un singolo comando.

È possibile configurare Access Guard a livello di storage, un altro livello di sicurezza applicato da ONTAP ai volumi SVM. Storage-Level Access Guard si applica agli accessi da tutti i protocolli NAS all'oggetto storage a cui è applicato Storage-Level Access Guard.

Access Guard a livello di storage può essere configurato e gestito solo dalla CLI di ONTAP. Non è possibile gestire le impostazioni di Storage-Level Access Guard dai client SMB. Inoltre, se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, non viene visualizzata la protezione Storage-Level Access Guard. La protezione di Storage-Level Access Guard non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX). Pertanto, Storage-Level Access Guard offre un ulteriore livello di sicurezza per l'accesso ai dati, impostato e gestito in modo indipendente dall'amministratore dello storage.

> Anche se sono supportate solo le autorizzazioni di accesso NTFS per Storage-Level Access Guard, ONTAP può eseguire controlli di sicurezza per l'accesso via NFS ai dati sui volumi in cui viene applicato Storage-Level Access Guard se l'utente UNIX esegue il mapping a un utente Windows sulla SVM proprietaria del volume.

Volumi NTFS di tipo Security

Tutti i file e le cartelle contenuti nei volumi e nei qtree di sicurezza NTFS dispongono di un'efficace protezione NTFS. È possibile utilizzare `vserver security file-directory` Famiglia di comandi per implementare i seguenti tipi di protezione sui volumi NTFS di tipo Security:

- Permessi dei file e policy di controllo per file e cartelle contenuti nel volume
- Protezione degli accessi a livello di storage sui volumi

Volumi misti di sicurezza

I volumi e i qtree misti in stile di sicurezza possono contenere alcuni file e cartelle con una protezione efficace UNIX e che utilizzano autorizzazioni per i file UNIX, i criteri di controllo Mbit di modalità o ACL NFSv4.x e NFSv4.x, nonché alcuni file e cartelle con una protezione effettiva NTFS e che utilizzano le autorizzazioni per i file NTFS e i criteri di controllo. È possibile utilizzare `vserver security file-directory` famiglia di

comandi per applicare i seguenti tipi di protezione a dati misti di tipo sicurezza:

- Permessi dei file e policy di controllo per file e cartelle con NTFS efficace in stile di sicurezza nel volume misto o nel qtree
- Access Guard a livello di storage per i volumi con sicurezza efficace NTFS e UNIX

Volumi UNIX di tipo Security

I volumi e le qtree UNIX di sicurezza contengono file e cartelle con protezione efficace UNIX (ovvero i bit di modalità o gli ACL NFSv4.x). Se si desidera utilizzare il, tenere presente quanto segue `vserver security file-directory` Famiglia di comandi per implementare la sicurezza su volumi UNIX di tipo Security:

- Il `vserver security file-directory` La famiglia di comandi non può essere utilizzata per gestire la sicurezza dei file UNIX e le policy di controllo su qtree e volumi di sicurezza UNIX.
- È possibile utilizzare `vserver security file-directory` Famiglia di comandi per configurare Storage-Level Access Guard su volumi UNIX di tipo Security, a condizione che SVM con il volume di destinazione contenga un server CIFS.

Informazioni correlate

Visualizza informazioni sulla sicurezza dei file e sulle policy di audit

Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI

Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la CLI

Proteggere l'accesso ai file utilizzando Storage-Level Access Guard

Casi di utilizzo dell'interfaccia CLI per impostare la sicurezza di file e cartelle

Poiché è possibile applicare e gestire la sicurezza di file e cartelle in locale senza il coinvolgimento di un client remoto, è possibile ridurre significativamente il tempo necessario per impostare la protezione in blocco su un gran numero di file o cartelle.

È possibile utilizzare la CLI per impostare la sicurezza di file e cartelle nei seguenti casi di utilizzo:

- Storage di file in ambienti aziendali di grandi dimensioni, ad esempio lo storage di file nelle home directory
- Migrazione dei dati
- Modifica del dominio Windows
- Standardizzazione delle policy di controllo e sicurezza dei file nei file system NTFS

Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle

È necessario conoscere alcuni limiti quando si utilizza la CLI per impostare la sicurezza di file e cartelle.

- Il `vserver security file-directory` La famiglia di comandi non supporta l'impostazione degli ACL

NFSv4.

È possibile applicare i descrittori di protezione NTFS solo a file e cartelle NTFS.

Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle

I descrittori di protezione contengono gli elenchi di controllo degli accessi che determinano le azioni che un utente può eseguire su file e cartelle e le operazioni controllate quando un utente accede a file e cartelle.

- **Autorizzazioni**

  Le autorizzazioni sono consentite o negate dal proprietario di un oggetto e determinano le azioni che un oggetto (utenti, gruppi o oggetti computer) può eseguire su file o cartelle specifici.

- **Descrittori di sicurezza**

  I descrittori di protezione sono strutture di dati che contengono informazioni di sicurezza che definiscono le autorizzazioni associate a un file o a una cartella.

- **ACL (Access Control List)**

  Gli elenchi di controllo degli accessi sono gli elenchi contenuti in un descrittore di protezione che contengono informazioni sulle azioni che gli utenti, i gruppi o gli oggetti computer possono eseguire nel file o nella cartella a cui è applicato il descrittore di protezione. Il descrittore di protezione può contenere i seguenti due tipi di ACL:

  - DACL (Discretionary Access Control List)
  - SACL (System Access Control List)

- **Elenchi di controllo degli accessi discrezionali (DACL)**

  I DACL contengono l'elenco dei SIDS per gli utenti, i gruppi e gli oggetti computer ai quali è consentito o negato l'accesso per eseguire azioni su file o cartelle. I DACL contengono zero o più voci di controllo degli accessi (ACE).

- **System access control list (SACL)**

  I SACL contengono l'elenco di SIDS per gli utenti, i gruppi e gli oggetti computer per i quali vengono registrati eventi di controllo riusciti o non riusciti. I SACL contengono zero o più voci di controllo degli accessi (ACE).

- **Voci di controllo di accesso (ACE)**

  Gli assi sono singole voci in DACL o SACL:

  - Una voce di controllo dell'accesso DACL specifica i diritti di accesso consentiti o negati per determinati utenti, gruppi o oggetti computer.
  - Una voce di controllo dell'accesso SACL specifica gli eventi di successo o di errore da registrare quando si controllano le azioni specifiche eseguite da utenti, gruppi o oggetti computer specifici.

- **Ereditarietà delle autorizzazioni**

L'ereditarietà delle autorizzazioni descrive il modo in cui le autorizzazioni definite nei descrittori di protezione vengono propagate a un oggetto da un oggetto padre. Solo le autorizzazioni ereditabili vengono ereditate dagli oggetti figlio. Quando si impostano le autorizzazioni sull'oggetto padre, è possibile decidere se cartelle, sottocartelle e file possono ereditare tali autorizzazioni con "applicabile a. `this-folder`, `sub-folders`e `files`".

Informazioni correlate

"Controllo SMB e NFS e tracciamento della sicurezza"

Configurazione e applicazione dei criteri di controllo a file e cartelle NTFS mediante l'interfaccia CLI

Linee guida per l'applicazione di policy di directory di file che utilizzano utenti o gruppi locali sulla destinazione di disaster recovery SVM

Prima di applicare i criteri di directory dei file alla destinazione di disaster recovery SVM (Storage Virtual Machine) in una configurazione di eliminazione dell'ID, è necessario tenere presenti alcune linee guida se la configurazione dei criteri di directory dei file utilizza utenti o gruppi locali nel descrittore di protezione o nelle voci DACL o SACL.

È possibile configurare una configurazione di disaster recovery per una SVM in cui la SVM di origine sul cluster di origine replica i dati e la configurazione dalla SVM di origine a una SVM di destinazione su un cluster di destinazione.

È possibile configurare uno dei due tipi di disaster recovery SVM:

- Identità preservata

  Con questa configurazione, l'identità di SVM e del server CIFS viene preservata.

- Identità scartata

  Con questa configurazione, l'identità di SVM e del server CIFS non viene preservata. In questo scenario, il nome di SVM e del server CIFS sulla SVM di destinazione è diverso da SVM e dal nome del server CIFS sulla SVM di origine.

Linee guida per le configurazioni di identità scartate

In una configurazione con eliminazione dell'identità, per un'origine SVM che contiene configurazioni di utente, gruppo e privilegi locali, il nome del dominio locale (nome del server CIFS locale) deve essere modificato in modo che corrisponda al nome del server CIFS sulla destinazione SVM. Ad esempio, se il nome SVM di origine è "vs1" e il nome del server CIFS è "CIFS1" e il nome SVM di destinazione è "vs1_dst" e il nome del server CIFS è "CIFS1_DST", il nome del dominio locale di un utente locale denominato "CIFS1` user1" viene automaticamente modificato in "`CIFST_DVM_1".

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Anche se i nomi degli utenti e dei gruppi locali vengono modificati automaticamente nei database degli utenti e dei gruppi locali, i nomi degli utenti o dei gruppi locali non vengono modificati automaticamente nelle configurazioni dei criteri delle directory dei file (criteri configurati sulla CLI tramite `vserver security file-directory` famiglia di comandi).

Ad esempio, per “vs1”, se è stata configurata una voce DACL in cui si trova `-account` Il parametro è impostato su "`CIFS1` user1", l’impostazione non viene modificata automaticamente sulla SVM di destinazione per riflettere il nome del server CIFS di destinazione.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

È necessario utilizzare `vserver security file-directory modify` Comandi per modificare manualmente il nome del server CIFS nel nome del server CIFS di destinazione.

Componenti di configurazione dei criteri di directory dei file che contengono parametri dell'account

Esistono tre componenti di configurazione dei criteri di directory dei file che possono utilizzare le impostazioni dei parametri che possono contenere utenti o gruppi locali:

- Descrittore di sicurezza

  È possibile specificare il proprietario del descrittore di protezione e il gruppo primario del proprietario del descrittore di protezione. Se il descrittore di protezione utilizza un utente o un gruppo locale per le voci del proprietario e del gruppo primario, è necessario modificare il descrittore di protezione per utilizzare la SVM di destinazione nel nome dell'account. È possibile utilizzare `vserver security file-directory ntfs modify` per apportare le modifiche necessarie ai nomi degli account.

- Voci DACL

  Ogni voce DACL deve essere associata a un account. Per utilizzare il nome SVM di destinazione, è necessario modificare tutti i DACL che utilizzano account utente o di gruppo locali. Poiché non è possibile modificare il nome dell'account per le voci DACL esistenti, è necessario rimuovere eventuali voci DACL con utenti o gruppi locali dai descrittori di protezione, creare nuove voci DACL con i nomi account di destinazione corretti e associare queste nuove voci DACL ai descrittori di protezione appropriati.

- Voci SACL

  Ogni voce SACL deve essere associata a un account. Per utilizzare il nome SVM di destinazione, è

necessario modificare tutti i SACL che utilizzano account utente o di gruppo locali. Poiché non è possibile modificare il nome dell'account per le voci SACL esistenti, è necessario rimuovere eventuali voci SACL con utenti o gruppi locali dai descrittori di protezione, creare nuove voci SACL con i nomi account di destinazione corretti e associare queste nuove voci SACL ai descrittori di protezione appropriati.

Prima di applicare il criterio, è necessario apportare le modifiche necessarie agli utenti o ai gruppi locali utilizzati nella configurazione del criterio della directory dei file; in caso contrario, il processo di applicazione non riesce.

Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI

Creare un descrittore di protezione NTFS

La creazione di un descrittore di sicurezza NTFS (policy di sicurezza dei file) è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo degli accessi NTFS (ACL) a file e cartelle che risiedono nelle macchine virtuali di storage (SVM). È possibile associare il descrittore di protezione al percorso di file o cartelle in un'attività di policy.

A proposito di questa attività

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

Oggetto	Tipo di accesso	Diritti di accesso	Dove applicare le autorizzazioni
BUILTIN/amministratori	Consentire	Controllo completo	questa-cartella, sottocartelle, file
BUILTIN/utenti	Consentire	Controllo completo	questa-cartella, sottocartelle, file
PROPRIETARIO DEL CREATOR	Consentire	Controllo completo	questa-cartella, sottocartelle, file
AUTORITÀ/SISTEMA NT	Consentire	Controllo completo	questa-cartella, sottocartelle, file

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario

- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Aggiungere le voci di controllo dell'accesso DACL NTFS al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) al descrittore di protezione NTFS è il secondo passo nella configurazione e nell'applicazione di ACL NTFS a un file o a una cartella. Ciascuna voce identifica l'oggetto a cui è consentito o negato l'accesso e definisce le operazioni che l'oggetto può o non può eseguire nei file o nelle cartelle definiti nell'ACE.

A proposito di questa attività

È possibile aggiungere uno o più ACE al DACL del descrittore di protezione.

Se il descrittore di protezione contiene un DACL con ACE esistenti, il comando aggiunge il nuovo ACE al DACL. Se il descrittore di protezione non contiene un DACL, il comando crea il DACL e aggiunge il nuovo ACE.

È possibile personalizzare le voci DACL specificando i diritti che si desidera consentire o negare per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati
- Diritti raw (privilegio avanzato)

> Se non si specificano i diritti per la voce DACL, l'impostazione predefinita è impostare i diritti su `Full Control`.

È possibile personalizzare le voci DACL specificando come applicare l'ereditarietà.

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Aggiungere una voce DACL a un descrittore di protezione: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Verificare che la voce DACL sia corretta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                    Vserver: vs1
         Security Descriptor Name: sd1
                   Allow or Deny: deny
             Account Name or SID: DOMAIN\joe
                   Access Rights: full-control
          Advanced Access Rights: -
                        Apply To: this-folder
                   Access Rights: full-control
```

Creare policy di sicurezza

La creazione di una policy di sicurezza dei file per le SVM è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare i criteri di protezione a ogni SVM (contenente volumi di sicurezza NTFS o volumi di sicurezza misti).

Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

  Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

  Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

  Anche se un criterio può contenere più attività, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

  Non assegnerà mai autorizzazioni di accesso aggiuntive.

Quando si aggiungono attività ai criteri di protezione, è necessario specificare i seguenti quattro parametri richiesti:

- Nome SVM
- Nome policy
- Percorso
- Descrittore di sicurezza da associare al percorso

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Applicare le policy di sicurezza

L'applicazione di una policy di sicurezza dei file alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

A proposito di questa attività

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).

> Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Fase

1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verificare la sicurezza del file applicata

È possibile verificare le impostazioni di sicurezza del file per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione abbiano le impostazioni desiderate.

A proposito di questa attività

Specificare il nome della SVM contenente i dati e il percorso del file e delle cartelle in cui si desidera verificare le impostazioni di sicurezza. È possibile utilizzare il opzionale `-expand-mask` per visualizzare informazioni dettagliate sulle impostazioni di sicurezza.

Fase

1. Visualizzare le impostazioni di sicurezza di file e cartelle: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

```
vserver security file-directory show -vserver vs1 -path /data/engineering
-expand-mask true
```

```
          Vserver: vs1
               File Path: /data/engineering
       File Inode Number: 5544
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
```

```
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
```

```
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la panoramica CLI

È necessario eseguire diversi passaggi per applicare i criteri di controllo a file e cartelle NTFS quando si utilizza l'interfaccia utente di ONTAP. Innanzitutto, si crea un descrittore di protezione NTFS e si aggiungono SACL al descrittore di protezione. Quindi, creare una policy di sicurezza e aggiungere attività di policy. Quindi, applicare il criterio di protezione a una macchina virtuale di storage (SVM).

A proposito di questa attività

Dopo aver applicato il criterio di protezione, è possibile monitorare il processo di criteri di protezione e verificare le impostazioni per il criterio di controllo applicato.

Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Informazioni correlate

Protezione dell'accesso ai file mediante Storage-Level Access Guard

Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle

Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle

"Controllo SMB e NFS e tracciamento della sicurezza"

Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI

Creare un descrittore di protezione NTFS

La creazione di un criterio di audit del descrittore di protezione NTFS è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo di accesso (ACL) NTFS a file e cartelle che risiedono all'interno delle SVM. Il descrittore di protezione verrà associato al percorso del file o della cartella in un'attività di policy.

A proposito di questa attività

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

Oggetto	Tipo di accesso	Diritti di accesso	Dove applicare le autorizzazioni
BUILTIN/amministratori	Consentire	Controllo completo	questa-cartella, sottocartelle, file
BUILTIN/utenti	Consentire	Controllo completo	questa-cartella, sottocartelle, file
PROPRIETARIO DEL CREATOR	Consentire	Controllo completo	questa-cartella, sottocartelle, file
AUTORITÀ/SISTEMA NT	Consentire	Controllo completo	questa-cartella, sottocartelle, file

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario

- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Se si desidera utilizzare i parametri avanzati, impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Creare un descrittore di sicurezza: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Verificare che la configurazione del descrittore di protezione sia corretta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                       Vserver: vs1
                               Security Descriptor Name: sd1
                        Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Se si è nel livello di privilegio avanzato, tornare al livello di privilegio admin: `set -privilege admin`

Aggiungere le voci di controllo dell'accesso NTFS SACL al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) SACL (elenco di controllo di accesso al sistema) al descrittore di protezione NTFS è la seconda fase della creazione di criteri di controllo NTFS per file o cartelle in SVM. Ogni voce identifica l'utente o il gruppo che si desidera controllare. La voce SACL definisce se si desidera controllare i tentativi di accesso riusciti o non riusciti.

A proposito di questa attività

È possibile aggiungere uno o più ACE al SACL del descrittore di protezione.

Se il descrittore di protezione contiene un SACL con ACE esistenti, il comando aggiunge il nuovo ACE al SACL. Se il descrittore di protezione non contiene un SACL, il comando crea il SACL e aggiunge il nuovo ACE.

È possibile configurare le voci SACL specificando i diritti da controllare per gli eventi di successo o di errore per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati

- Diritti raw (privilegio avanzato)

> Se non si specificano i diritti per la voce SACL, l'impostazione predefinita è `Full Control`.

È possibile personalizzare le voci SACL specificando come applicare l'ereditarietà con `apply to` parametro. Se non si specifica questo parametro, l'impostazione predefinita prevede l'applicazione di questa voce SACL a questa cartella, sottocartelle e file.

Fasi

1. Aggiungere una voce SACL a un descrittore di protezione: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Verificare che la voce SACL sia corretta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                   Vserver: vs1
                     Security Descriptor Name: sd1
         Access type for Specified Access Rights: failure
                         Account Name or SID: DOMAIN\joe
                               Access Rights: full-control
                      Advanced Access Rights: -
                                   Apply To: this-folder
                               Access Rights: full-control
   ```

Creare policy di sicurezza

La creazione di un criterio di audit per le macchine virtuali di storage (SVM) è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare la policy di sicurezza a ciascuna macchina virtuale di storage (SVM) (contenente volumi di sicurezza NTFS o volumi misti di sicurezza).

Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

  Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

  Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

  Anche se un criterio può contenere più attività, non è possibile configurare un criterio in modo che

contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

  Non assegnerà mai autorizzazioni di accesso aggiuntive.

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

Fasi

1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Applicare le policy di sicurezza

L'applicazione di un criterio di audit alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

A proposito di questa attività

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).

> Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

Fase

1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 –id 53322" command to view the status of the operation
   ```

Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

Verificare la policy di audit applicata

È possibile verificare il criterio di controllo per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione dispongano delle impostazioni di sicurezza di controllo desiderate.

A proposito di questa attività

Si utilizza `vserver security file-directory show` comando per visualizzare le informazioni sui criteri di controllo. Specificare il nome della SVM che contiene i dati e il percorso dei dati di cui si desidera visualizzare le informazioni sui criteri di controllo del file o della cartella.

Fase

1. Visualizzare le impostazioni dei criteri di controllo: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Esempio

Il seguente comando visualizza le informazioni di policy di audit applicate al percorso “/corp” in SVM vs1. Il percorso ha applicato sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerazioni per la gestione dei processi di policy di sicurezza

Se esiste un processo di policy di sicurezza, in determinate circostanze non è possibile modificare tale policy o le attività assegnate a tale policy. È necessario comprendere in quali condizioni è possibile o meno modificare le policy di sicurezza in modo che i tentativi di modifica vengano eseguiti correttamente. Le modifiche al criterio includono l'aggiunta, la rimozione o la modifica delle attività assegnate al criterio e l'eliminazione o la modifica del criterio.

Non è possibile modificare un criterio di protezione o un'attività assegnata a tale criterio se esiste un processo per tale criterio e tale processo si trova nei seguenti stati:

- Il lavoro è in esecuzione o in corso.
- Il processo viene messo in pausa.
- Il lavoro viene ripreso e si trova in esecuzione.
- Se il processo è in attesa di eseguire il failover su un altro nodo.

Nei seguenti casi, se esiste un processo per un criterio di protezione, è possibile modificare correttamente tale criterio di protezione o un'attività assegnata a tale criterio:

- Il processo di policy viene arrestato.
- Il processo di policy è stato completato correttamente.

Comandi per la gestione dei descrittori di sicurezza NTFS

Esistono comandi ONTAP specifici per la gestione dei descrittori di protezione. È possibile creare, modificare, eliminare e visualizzare informazioni sui descrittori di protezione.

Se si desidera…	Utilizzare questo comando…
Creare descrittori di protezione NTFS	`vserver security file-directory ntfs create`
Modificare i descrittori di protezione NTFS esistenti	`vserver security file-directory ntfs modify`
Visualizza informazioni sui descrittori di protezione NTFS esistenti	`vserver security file-directory ntfs show`
Eliminare i descrittori di protezione NTFS	`vserver security file-directory ntfs delete`

Vedere le pagine man per `vserver security file-directory ntfs` per ulteriori informazioni.

Comandi per la gestione delle voci di controllo degli accessi NTFS DACL

Esistono comandi ONTAP specifici per la gestione delle voci di controllo degli accessi DACL (Access Control). È possibile aggiungere ACE ai DACL NTFS in qualsiasi momento. È inoltre possibile gestire i DACL NTFS esistenti modificando, eliminando e visualizzando le informazioni relative agli ACE nei DACL.

Se si desidera…	Utilizzare questo comando…
Creare ACE e aggiungerli ai DACL NTFS	`vserver security file-directory ntfs dacl add`
Modificare gli ACE esistenti nei DACL NTFS	`vserver security file-directory ntfs dacl modify`

Se si desidera…	Utilizzare questo comando…
Visualizza le informazioni sugli ACE esistenti nei DACL NTFS	`vserver security file-directory ntfs dacl show`
Rimuovere gli ACE esistenti dai DACL NTFS	`vserver security file-directory ntfs dacl remove`

Vedere le pagine man per `vserver security file-directory ntfs dacl` per ulteriori informazioni.

Comandi per la gestione delle voci di controllo degli accessi NTFS SACL

Esistono comandi ONTAP specifici per la gestione delle voci di controllo degli accessi SACL (ACE). È possibile aggiungere ACE ai SACL NTFS in qualsiasi momento. È inoltre possibile gestire i SACL NTFS esistenti modificando, eliminando e visualizzando le informazioni relative agli ACE nei SACL.

Se si desidera…	Utilizzare questo comando…
Creare ACE e aggiungerli ai SACL NTFS	`vserver security file-directory ntfs sacl add`
Modificare gli ACE esistenti nei SACL NTFS	`vserver security file-directory ntfs sacl modify`
Visualizza le informazioni sugli ACE esistenti nei SACL NTFS	`vserver security file-directory ntfs sacl show`
Rimuovere gli ACE esistenti dai SACL NTFS	`vserver security file-directory ntfs sacl remove`

Vedere le pagine man per `vserver security file-directory ntfs sacl` per ulteriori informazioni.

Comandi per la gestione delle policy di sicurezza

Esistono comandi ONTAP specifici per la gestione delle policy di sicurezza. È possibile visualizzare informazioni sui criteri ed eliminare i criteri. Non è possibile modificare un criterio di protezione.

Se si desidera…	Utilizzare questo comando…
Creare policy di sicurezza	`vserver security file-directory policy create`

Se si desidera…	Utilizzare questo comando…
Visualizzare informazioni sulle policy di sicurezza	`vserver security file-directory policy show`
Eliminare le policy di sicurezza	`vserver security file-directory policy delete`

Vedere le pagine man per `vserver security file-directory policy` per ulteriori informazioni.

Comandi per la gestione delle attività dei criteri di protezione

Sono disponibili comandi ONTAP per aggiungere, modificare, rimuovere e visualizzare informazioni sulle attività dei criteri di protezione.

Se si desidera…	Utilizzare questo comando…
Aggiungere attività di policy di sicurezza	`vserver security file-directory policy task add`
Modificare le attività dei criteri di protezione	`vserver security file-directory policy task modify`
Visualizza informazioni sulle attività dei criteri di protezione	`vserver security file-directory policy task show`
Rimuovere le attività dei criteri di protezione	`vserver security file-directory policy task remove`

Vedere le pagine man per `vserver security file-directory policy task` per ulteriori informazioni.

Comandi per la gestione dei processi di policy di sicurezza

Sono disponibili comandi ONTAP per mettere in pausa, riprendere, arrestare e visualizzare informazioni sui processi relativi ai criteri di protezione.

Se si desidera…	Utilizzare questo comando…
Sospendere i processi di policy di sicurezza	`vserver security file-directory job pause -vserver vserver_name -id integer`
Riprendere i processi di policy di sicurezza	`vserver security file-directory job resume -vserver vserver_name -id integer`

Se si desidera…	Utilizzare questo comando…
Visualizza informazioni sui processi di policy di sicurezza	`vserver security file-directory job show -vserver vserver_name` È possibile determinare l'ID lavoro di un lavoro utilizzando questo comando.
Arrestare i processi di policy di sicurezza	`vserver security file-directory job stop -vserver vserver_name -id integer`

Vedere le pagine man per `vserver security file-directory job` per ulteriori informazioni.